

IN THE CLAIMS:

Please amend claims 12 and 27 as follows:

1 – 11. (canceled)

12. (currently amended) A method for limiting the operational life of software in a network environment, the method comprising:

transmitting a program applet with a password embedded ~~therewithin~~ therein from a server computer to a client computer, via a network, the password having a limited operational life, and the program applet including executable code that runs on the client computer;

receiving by the server computer, from said program applet running on the client computer, via said network, (i) a request for information stored in a restricted access storage area of the server computer, and (ii) said embedded password;

authenticating said embedded password by the server computer, whenever said receiving occurs;

thereafter transmitting said information from the server computer, to said program applet running on the client computer, via said network, while said embedded password is valid; and

invalidating said embedded password by the server computer, coincident with an invalidation event.

13. (previously presented) A method according to claim **12** wherein said invalidating comprises invalidating said embedded password at a predetermined time.

14. (previously presented) A method according to claim **12** wherein said invalidating comprises invalidating said embedded password after lapse of a predetermined time from when said request was received.

15. (previously presented) A method according to claim **12** wherein said invalidating comprises invalidating said embedded password upon the detection of a loss of communication with said client.

16. (canceled)

17. (canceled)

18. (previously presented) A method according to claim **12** wherein said transmitting a program applet comprises generating said embedded password.

19. – 26. (canceled)

27. (currently amended) A network-based software authentication system comprising a server computer, the server computer comprising:

- a password generator;
- password validation apparatus;
- a restricted-access storage area;
- a program applet including executable code that runs on a client computer; and

- invalidation apparatus;

wherein said server computer is operative to:

- a) cause said password generator to generate a password, the password having a limited operational life;

- b) embed said password within said program applet, and transmit said program applet with said password embedded ~~therewithin~~ therein to the client computer via a network;

- c) receive from said program applet running on the client computer, (i) a request for information, and (ii) said embedded password for authentication;

- d) authenticate said embedded password using said password validation apparatus, whenever information requested is stored in the restricted-access storage area;

e) transmit said information to said program applet running on the client computer, via said network, while said embedded password is valid; and
f) invalidate said embedded password using said invalidation apparatus coincident with an invalidation event.

28. (original) A system according to claim **27** wherein said invalidation event comprises the arrival of a predetermined time.

29. (previously presented) A system according to claim **27** wherein said invalidation event comprises the lapsing of a predetermined time from when said request was received.

30. (original) A system according to claim **27** wherein said invalidation event comprises the detection of a loss of communication with said client.

31. (canceled)

32. (canceled)

33. (canceled)